Universally Attainable Error and Information Exponents, and Equivocation Rate for the Broadcast Channels with Confidential Messages

Masahito Hayashi
Graduate School of Information Sciences,
Tohoku University, 980-8579 Japan
and Centre for Quantum Technologies,
National University of Singapore,
3 Science Drive 2, Singapore 117542

Ryutaroh Matsumoto
Department of Communications and Integrated Systems,
Tokyo Instiutte of Technology, 152-8550 Japan

***Abstract*—We show universally attainable exponents for the decoding error and the mutual information and universally attainable equivocation rates for the conditional entropy for the broadcast channels with confidential messages. The error exponents are the same as ones given by Körner and Sgarro for the broadcast channels with degraded message sets.**

***Index Terms*—broadcast channel with confidential messages, information theoretic security, multiuser information theory**

I. Introduction

The information theoretic security attracts much attention recently [13], because it offers security that does not depend on a conjectured difficulty of some computational problem. A classical problem in the information theoretic security is the broadcast channel with confidential messages (hereafter abbreviated as BCC) first considered by Csiszár and Körner [5], in which there is a single sender called Alice and two receivers called Bob and Eve. The problem in [5] is a generalization of the wiretap channel considered by Wyner [18]. In the formulation in [5], Alice has a common messages destined for both Bob and Eve and a private message destined solely for Bob. The word “confidential” means that Alice wants to prevent Eve from knowing much about the private message. The coding in this situation has two goals, namely error correction and secrecy. The degree of secrecy is measured by the mutual information between the private message to Bob and the received signal by Eve.

On the other hand, the broadcast channel with degraded message sets (hereafter abbreviated as BCD), considered by Körner and Marton [11], is a special case of BCC in which there is no requirement on the confidentiality of the private message to Bob. Körner and Sgarro [10] proposed the universal encoder and decoder for BCD, which did not use conditional probability distribution of the channel for encoding nor decoding, and clarified universally attainable error exponents for BCD. In studies of universal coding for channels, we consider the compound channel, which is a collection of (usually infinitely many) channels and try to clarify the exponents realized by given encoder and decoder over that collection of channels. The capacity of the compound wiretap channel was studied by Liang et al. [12], in which the number of channels is finite and the receiver is assumed to know the conditional probability distribution of the channel. Kobayashi et al. [9] studied the BCC under the same assumption as [12]. The assumption in [9], [12] is more restrictive than [10] and they [9], [12] only proved that the mutual information divided by the code length converges to zero, which means that their universally attainable information exponents are zero.

In contrast to them, Soma [17] clarified the universally attainable information exponents for the wiretap channels under the same assumption as [10], though he did not analyze the universally attainable error exponent by his coding scheme. Soma [17] used the channel resolvability lemma in [7], and it was totally unclear how to extend his argument to the BCC with common messages. Soma did not clarified the speed of convergence of mutual information to the infinity when the information rate of private message is large, neither. We note that our universally attainable information exponent is the same as Soma’s [17] when there is no common message.

In this paper, we attach the two-universal hash functions [2] to the encoder proposed by Körner and Sgarro [10], then we use the privacy amplification theorem [1] for the analysis of the mutual information to obtain the universally attainable error and information exponents and universally attainable equivocation rates for the BCC. Our argument is similar to the non-universal coding considered in [15] and the secure multiplex coding considered in [14].

This paper is organized as follows: Section II reviews relevant research results used in this paper. Section III introduces the definition of universally attainable exponents and provides ones satisfying the definition. Section IV concludes the paper.

II. Preliminary

A. Broadcast channels with confidential messages

Let Alice, Bob, and Eve be as defined in Section I. $\mathcal{X}$ denotes the channel input alphabet and $\mathcal{Y}$ (resp. $\mathcal{Z}$) denotes the channel output alphabet to Bob (resp. Eve). We assume that

$\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ are finite unless otherwise stated. We denote the conditional probability of the channel to Bob (resp. Eve) by $P_{Y|X}$ (resp. $P_{Z|X}$). The set $\mathcal{S}_n$ denotes that of the secret message and $\mathcal{E}_n$ does that of the common message when the block coding of length n is used. We shall define the achievability of a rate triple (R_s, R_e, R_c). For the notational convenience, we fix the base of logarithm, including one used in entropy and mutual information, to the base of natural logarithm. The privacy amplification theorem introduced in Theorem 6 is sensitive to choice of the base of logarithm.

Definition 1: The rate triple (R_s, R_e, R_c) is said to be *achievable* if there exists a sequence of Alice's stochastic encoder f_n from $\mathcal{S}_n \times \mathcal{E}_n$ to $\mathcal{X}^n$, Bob's deterministic decoder $\varphi_n : \mathcal{Y}^n \to \mathcal{S}_n \times \mathcal{E}_n$ and Eve's deterministic decoder $\psi_n : \mathcal{Z}^n \to \mathcal{E}_n$ such that

$$\begin{aligned}
\lim_{n\to\infty} \Pr[(S_n, E_n) \neq \varphi_n(Y^n) \text{ or } E_n \neq \psi_n(Z^n)] &= 0,\\
\liminf_{n\to\infty} \frac{H(S_n|Z^n)}{n} &\geq R_e,\\
\liminf_{n\to\infty} \frac{\log|\mathcal{S}_n|}{n} &\geq R_\mathrm{s},\\
\liminf_{n\to\infty} \frac{\log|\mathcal{E}_n|}{n} &\geq R_\mathrm{c},
\end{aligned}$$

where S_n and E_n represents the secret and the common message, respectively, have the uniform distribution on $\mathcal{S}_n$ and $\mathcal{E}_n$, respectively, and Y^n and Z^n are the received signal by Bob and Eve, respectively, with the transmitted signal $f_n(S_n, E_n)$ and the channel transition probabilities $P_{Y|X}$, $P_{Z|X}$. The capacity region of the BCC is the closure of the achievable rate triples.

Theorem 2: [5] The capacity region for the BCC is given by the set of R_c, R_s and R_e such that there exists a Markov chain $U \to V \to X \to YZ$ and

$$\begin{aligned}
R_\mathrm{s} + R_\mathrm{c} &\leq I(V;Y|U) + \min[I(U;Y), I(U;Z)], &(1)\\
R_\mathrm{c} &\leq \min[I(U;Y), I(U;Z)], &(2)\\
R_e &\leq I(V;Y|U) - I(V;Z|U),\\
R_e &\leq R_\mathrm{s}.
\end{aligned}$$

As described in [13], U can be regarded as the common message, V the combination of the common and the private messages, and X the transmitted signal.

Corollary 3: [5] The notation is same as Theorem 2. If we require $R_e = R_\mathrm{s}$, the capacity region for (R_c, R_s) is given by the set of R_c and R_s such that there exists a Markov chain $U \to V \to X \to YZ$ and

$$\begin{aligned}
R_\mathrm{c} &\leq \min[I(U;Y), I(U;Z)],\\
R_\mathrm{s} &\leq I(V;Y|U) - I(V;Z|U).
\end{aligned}$$

B. Broadcast channels with degraded message sets

If we set $R_e = 0$ in the BCC, the secrecy requirement is removed from BCC, and the coding problem is equivalent to the broadcast channel with degraded message sets (abbreviated as BCD) considered by Körner and Marton [11].

Corollary 4: The capacity region of the BCD is given by the set of R_c and R_p such that there exists a Markov chain $U \to V = X \to YZ$ and

$$\begin{aligned}
R_\mathrm{c} &\leq \min[I(U;Y), I(U;Z)],\\
R_\mathrm{c} + R_\mathrm{p} &\leq I(V;Y|U) + \min[I(U;Y), I(U;Z)], &(3)
\end{aligned}$$

where R_p denotes the rate of the private message.

C. Two-universal hash functions

We shall use a family of two-universal hash functions [2] for the privacy amplification theorem introduced later.

Definition 5: Let $\mathcal{F}$ be a set of functions from $\mathcal{S}_1$ to $\mathcal{S}_2$, and F the not necessarily uniform random variable on $\mathcal{F}$. If for any $x_1 \neq x_2 \in \mathcal{S}_1$ we have

$$\Pr[F(x_1) = F(x_2)] \leq \frac{1}{|\mathcal{S}_2|},$$

then $\mathcal{F}$ is said to be a *family of two-universal hash functions*.

D. Strengthened privacy amplification theorem

In order to analyze the equivocation rate, we need to strengthen the privacy amplification theorem originally appeared in [1], [8].

Theorem 6: [14], [16] Let L be a random variable with a finite alphabet $\mathcal{L}$ and Z any random variable. Let $\mathcal{F}$ be a family of two-universal hash functions from $\mathcal{L}$ to $\mathcal{M}$, and F be a random variable on $\mathcal{F}$ statistically independent of L. Then

$$\mathbf{E}_f \exp(\rho I(F(L); Z|F = f)) \leq 1 + |\mathcal{M}|^\rho \mathbf{E}[P_{L|Z}(L|Z)^\rho] \qquad (4)$$

for $0 < \rho \leq 1$.

In addition to the above assumptions, when L is uniformly distributed, we have

$$|\mathcal{M}|^\rho \mathbf{E}[P_{L|Z}(L|Z)^\rho] = \frac{|\mathcal{M}|^\rho \mathbf{E}[P_{L|Z}(L|Z)^\rho P_L(L)^{-\rho}]}{|\mathcal{L}|^\rho}. \qquad (5)$$

In addition to all of the above assumptions, when Z is a discrete random variable, we have

$$\frac{|\mathcal{M}|^\rho \mathbf{E}[P_{L|Z}(L|Z)^\rho P_L(L)^{-\rho}]}{|\mathcal{L}|^\rho} = \frac{|\mathcal{M}|^\rho}{|\mathcal{L}|^\rho} \sum_{z,\ell} P_L(\ell) P_{Z|L}(z|\ell)^{1+\rho} P_Z(z)^{-\rho}. \qquad (6)$$

As in [8] we introduce the following two functions.

Definition 7:

$$\begin{aligned}
\psi(\rho, P_{Z|L}, P_L) &= \log \sum_z \sum_\ell P_L(\ell) P_{Z|L}(z|\ell)^{1+\rho} P_Z(z)^{-\rho}, &(7)\\
\phi(\rho, P_{Z|L}, P_L) &= \log \sum_z \left(\sum_\ell P_L(\ell) (P_{Z|L}(z|\ell)^{1/(1-\rho)}) \right)^{1-\rho} &(8)
\end{aligned}$$

Observe that ϕ is essentially Gallager's function E_0 [6].

At the end of our evaluation of the mutual information to Eve, we shall use the averaged version of ϕ, which is introduced below.

Definition 8:

$$\phi(\rho, P_{Z|L}, P_{L|U}, P_U)$$

$$= \quad \log \sum_u P_U(u) \sum_z \left(\sum_\ell P_{L|U}(\ell|u)(P_{Z|L}(z|\ell)^{1/(1-\rho)}) \right)^{1-\rho} \quad (9)$$

Proposition 9: For fixed $0 < \rho \leq 1$, P_L, $\tilde{P}_L$, $P_{Z|L}$, and $\tilde{P}_{Z|L}$ we have

$$\exp(\psi(\rho, P_{Z|L}, P_L)) \leq \exp(\phi(\rho, P_{Z|L}, P_L)). \quad (10)$$

$$\exp(\phi(\rho, P_{Z|L}, P_L)) \leq C_1 \exp(\phi(\rho, P_{Z|L}, \tilde{P}_L)) \quad (11)$$

when $P_L \leq C_1 \tilde{P}_L$.

Proof: The first inequality (10) was shown in [8].

Any positive concave function f of probability distributions satisfies

$$f(P) \leq \alpha f(Q), \quad (12)$$

when $P \leq \alpha \times Q$ with a positive real number $\alpha \geq 1$. This is because by the assumption there exists another distribution R such that $(1/\alpha)P + (\alpha - 1)/\alpha \cdot R = Q$, and

$$\begin{aligned} f(P)/\alpha &\leq f(P)/\alpha + (\alpha-1)/\alpha \cdot f(R) \\ &\leq f((1/\alpha)P + (\alpha-1)/\alpha \cdot R) = f(Q). \end{aligned}$$

Since $\exp(\phi(\rho, P_{Z|L}, P_L))$ is concave with respect to P_L with fixed $0 < \rho < 1$ and $P_{Z|L}$ [6], the second inequality (11) holds. ■

III. Universal coding for the broadcast channels with confidential messages

A. Universally attainable exponents and universally attainable equivocation rates

We introduce the universally attainable exponents for the BCC by adjusting the original definition for the BCD given by Körner and Sgarro [10].

Definition 10: Let $\mathcal{W}(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ be the set of all discrete memoryless broadcast channels $W : \mathcal{X} \to \mathcal{Y}, \mathcal{Z}$, and $\mathbf{R}^+$ the set of positive real numbers. A quadruple of functions ($\tilde{E}^{\mathrm{p}}$, $\tilde{E}^{\mathrm{c}}$, $\tilde{E}^{\mathrm{I}}_+$, $\tilde{E}^{\mathrm{I}}_-$) from $\mathbf{R}^+ \times \mathbf{R}^+ \times \mathcal{W}(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ to $[\mathbf{R}^+ \cup \{0\}]^4$ is said to be a universally attainable quadruple of exponents and equivocation rate for the family $\mathcal{W}(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ if, for every $R_{\mathrm{s}} > 0$, $R_{\mathrm{c}} > 0$, $\delta > 0$, and for sufficiently large n, there exists a sequence of codes (f_n, φ_n, ψ_n) of length n of rate pair at least (R_{s}, R_{c}) such that, denoting by $e^{\mathrm{s}}_n(W)$, $e^{\mathrm{c}}_n(W)$, $e^{\mathrm{I}}_n(W)$ the maximum error probabilities by Bob and by Eve and the mutual information between the secret message and Eve's received signal, for the n-th memoryless extension of the channel $W \in \mathcal{W}(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ we have

$$e^{\mathrm{s}}_n(W) \leq \exp(-n[\tilde{E}^{\mathrm{s}}(R_{\mathrm{s}}, R_{\mathrm{c}}) - \delta]), \quad (13)$$

$$e^{\mathrm{c}}_n(W) \leq \exp(-n[\tilde{E}^{\mathrm{c}}(R_{\mathrm{s}}, R_{\mathrm{c}}) - \delta]), \quad (14)$$

$$e^{\mathrm{I}}_n(W) \leq \max\{\exp(-n[\tilde{E}^{\mathrm{I}}_+(R_{\mathrm{s}}, R_{\mathrm{c}}) - \delta]), n[\tilde{E}^{\mathrm{I}}_-(R_{\mathrm{s}}, R_{\mathrm{c}}) + \delta]\}, \quad (15)$$

where R_{s} and R_{c} denote the rate of the secret message and the common message, respectively.

Suppose that we are given a broadcast $W : \mathcal{X} \to \mathcal{Y}, \mathcal{Z}$ and positive real numbers R_{s} and R_{c}. We fix a distribution Q_{UV} on $\mathcal{U} \times \mathcal{V}$, a channel $\Xi : \mathcal{V} \to \mathcal{X}$, and the rate R_{p} of the private message in the BCD encoder that satisfy Eqs. (1), (2) and (3), where the RVs U ,V, X, Y and Z in Eqs. (1), (2) and (3) are distributed according to Q_{UV}, Ξ and W. We present a universally attainable quadruple of exponents and equivocation rate in terms of R_{p}, Q_{UV} and Ξ as

$$F^{\mathrm{s}} = F^{\mathrm{s}}(W, R_{\mathrm{p}}, R_{\mathrm{c}}, Q_{UV}, \Xi) = F^{\mathcal{Y},\mathrm{KS}}(W \circ \Xi, R_{\mathrm{p}}, R_{\mathrm{c}}, Q_{UV}), \quad (16)$$

$$F^{\mathrm{c}} = F^{\mathrm{c}}(W, R_{\mathrm{p}}, R_{\mathrm{c}}, Q_{UV}, \Xi) = F^{\mathcal{Z},\mathrm{KS}}(W \circ \Xi, R_{\mathrm{p}}, R_{\mathrm{c}}, Q_{UV}), \quad (17)$$

$$\begin{aligned} F^{\mathcal{I}}_+ &= F^{\mathcal{I}}_+(W, R_{\mathrm{p}}, R_{\mathrm{s}}, Q_{UV}, \Xi) \\ &= \sup_{0<\rho\leq 1} \left[\rho(R_{\mathrm{p}} - R_{\mathrm{s}}) - \phi(\rho, W_{\mathcal{Z}} \circ \Xi, Q_{V|U}, Q_U) \right] \quad (18) \end{aligned}$$

$$F^{\mathcal{I}}_- = F^{\mathcal{I}}_-(W, R_{\mathrm{p}}, R_{\mathrm{s}}, Q_{UV}, \Xi) = I(V; Z|U) - R_{\mathrm{p}} + R_{\mathrm{s}}, \quad (19)$$

where $F^{\mathcal{Y},\mathrm{KS}}$ and $F^{\mathcal{Z},\mathrm{KS}}$ are the error exponent functions appeared in [10, Theorem 2].

Theorem 11 (Extension of [10, Theorem 1, part (a)]): Eqs. (16)–(19) are a universally attainable quadruple of exponents and equivocation rate in the sense of Definition 10. *Proof.* We shall attach the inverse of two-universal hash functions to the constant composition code used by Körner and Sgarro. We do not evaluate the decoding error probability, because that of our code is not larger than [10]. Observe that our exponents in Eqs. (16) and (17) are the same as [10] with the channel $W \circ \Xi$. We shall evaluate the mutual information.

We assume for a while that Q_{UV} is a type of a sequence of length n over $\mathcal{U} \times \mathcal{V}$. Recall that their codebook [10, Appendix] in the random coding is chosen according to the uniform distribution on the sequences with joint type Q_{UV}. Let n be the code length, $\mathcal{B}_n$ the set of private messages for the BCD encoder, and $\mathcal{E}_n$ the set of common messages. For $b \in \mathcal{B}_n$ and $e \in \mathcal{E}_n$, $\lambda(b, e) \in \mathcal{V}^n$ denotes the codeword of (b, e) encoded by the BCD encoder λ. Λ denotes the random selection of λ in the random coding argument.

Let $\mathcal{S}_n$ be the set of secret messages in the BCC. Let $\mathcal{F}_n$ be a family of two-universal hash functions from $\mathcal{B}_n$ to $\mathcal{S}_n$. For every $f \in \mathcal{F}_n$, we assume that f is surjective and that $f^{-1}(s)$ has the constant number of elements for every $s \in \mathcal{S}_n$. Those assumptions are met, for example, by choosing the set of all surjective linear maps from $\mathcal{B}_n$ to $\mathcal{S}_n$ as $\mathcal{F}_n$.

The structure of the transmitter and the receiver is as follows: Fix a hash function $f_n \in \mathcal{F}_n$ and Alice and Bob agree on the choice of f_n. Given a secret message s_n, choose b_n uniformly randomly from $\{b \in \mathcal{B}_n \mid f_n(b) = s_n\}$, treat b_n as the private message to Bob, encode b_n along with the common message e_n by a BCD encoder, and get a codeword v^n. Apply the artificial noise to v^n according to the conditional probability distribution Ξ and get the transmitted signal x^n. Bob decodes the received signal and get b_n, then apply f_n to b_n to get s_n. This construction requires Alice and Bob to agree on the choice of f_n.

Let S_n denote the RV of the secret message. Define B_n to be the RV uniformly chosen from the random set $\{b \in \mathcal{B}_n \mid F_n(b) = S_n\}$. In the following discussion, since we treat the channel $W^n_{\mathcal{Z}} \circ \Xi^n : \mathcal{V}^n \to \mathcal{Z}^n$, we simplify it to $\overline{W}^n_{\mathcal{Z}}$.

In this case, the mutual information between $F_n(B_n)$ and Z^n depends on the channel from $\mathcal{V}^n$ to $\mathcal{Z}^n$. In particular, for the later analysis, we need to treat the mutual information between $F_n(B_n)$ and Z^n when the channel from $\mathcal{V}^n$ to $\mathcal{Z}^n$ is not necessarily memoryless. So, the mutual information between $F_n(B_n)$ and Z^n will be written as a function $I_{\overline{W}_n}(F_n(B_n);Z^n|F_n)$ of a discrete channel $\overline{W}_n$ from $\mathcal{V}^n$ to $\mathcal{Z}^n$. Note that $\overline{W}_n$ is arbitrary and is not necessarily memoryless.

We want to apply the privacy amplification theorem in order to evaluate $I_{\overline{W}_n}(F_n(B_n);Z^n|F_n)$. To use the theorem we must ensure independence of F_n and B_n. The independence is satisfied by the assumptions on $\mathcal{F}_n$ if S_n is uniformly distributed. In that case B_n is uniformly distributed over $\mathcal{B}_n$. The remaining task is to find an upper bound on $I_{\overline{W}_n}(F_n(B_n);Z^n|F_n,\Lambda)$.

Firstly, we consider $\mathbf{E}_{f_n}\exp(\rho I_{W_n}(F_n(B_n);Z^n|F_n = f_n,\ \Lambda = \lambda))$ with fixed selection λ of Λ. In the following analysis, we do not make any assumption on the probability distribution of E_n except that S_n, E_n, F_n and Λ are statistically independent.

Recall that Λ is the RV indicating selection of codebook in the random ensemble constructed from the joint type Q_{UV} in the way considered in [10, Appendix]. Let $U^n = \Lambda(E_n)$ on $\mathcal{U}^n$ and $V^n = \Lambda(B_n,E_n)$ on $\mathcal{V}^n$ codewords for the BCD taking the random selection Λ taking into account, and Z^n Eve's received signal. Since we are using the constant composition code as used in [10], U^n and V^n are not i.i.d. RVs. So, the distribution P_{V^n,U^n} satisfies

$$P_{V^n|U^n=u}(v) \le (n+1)^{|\mathcal{U}\times\mathcal{V}|}Q^n_{V|U}(v|u) \qquad (20)$$

for a fixed $u\in\mathcal{U}^n$ by [3, Lemma 2.5, Chapter 1], and

$$P_{U^n}(u) \le (n+1)^{|\mathcal{U}|}Q^n_U(u), \qquad (21)$$

by [3, Lemma 2.3, Chapter 1]. Hence, (11) yields that

$$\begin{aligned}&\exp(\phi(\rho,\overline{W}^n_{\mathcal{Z}},P_{V^n|U^n},P_{U^n}))\\ \le&(n+1)^{|\mathcal{U}|^2|\mathcal{V}|}\exp(\phi(\rho,\overline{W}^n_{\mathcal{Z}},Q^n_{V|U},Q^n_U)).\end{aligned} \qquad (22)$$

In the code Λ, the random variable V^n takes values in the subset $T_n(Q_V)$, which is defined as the set of elements of $\mathcal{V}^n$ whose type is Q_V. Hence, it is sufficient to treat the channel whose input system is the subset $T_n(Q_V)$ of $\mathcal{V}^n$. Then, we have the following convex combination:

$$\overline{W}^n_{\mathcal{Z}}|_{T_n(Q_V)} = \sum_{\overline{W}_n\in\mathcal{W}_n(Q_V)}\lambda(\overline{W}_n)\overline{W}_n, \qquad (23)$$

where $\lambda(\overline{W}_n)$ is a positive constant and $\mathcal{W}_n(Q_V)$ is the family of conditional types from $\mathcal{V}^n$ to $\mathcal{Z}^n$, which is the V-shell of a sequence of type Q_V. The joint convexity of the conditional relative entropy yields that

$$I_{\overline{W}^n_{\mathcal{Z}}}(F_n(B_n);Z^n|F_n) \le \sum_{\overline{W}_n\in\mathcal{W}_n(Q_V)}\lambda(\overline{W}_n)I_{\overline{W}_n}(F_n(B_n);Z^n|F_n). \qquad (24)$$

We can also show that for any element $\overline{W}_n\in\mathcal{W}_n(Q_V)$ we have

$$\begin{aligned}&e^{\phi(\rho,\overline{W}^n_{\mathcal{Z}},P_{V^n|U^n},P_{U^n})}\\ =&\sum_u P_{U^n}(u)\sum_z(\sum_v P_{V^n|U^n}(v|u)(\sum_{\overline{W}'_n\in\mathcal{W}_n(Q_V)}\lambda(\overline{W}'_n)\overline{W}'_n(z|v))^{\frac{1}{1-\rho}})^{1-\rho}\\ \ge&\sum_u P_{U^n}(u)\sum_z(\sum_v P_{V^n|U^n}(v|u)(\lambda(\overline{W}_n)\overline{W}_n(z|v))^{\frac{1}{1-\rho}})^{1-\rho}\\ =&\lambda(\overline{W}_n)e^{\phi(\rho,\overline{W}_n,P_{V^n|U^n},P_{U^n})}.\end{aligned} \qquad (25)$$

Hence, in order to evaluate $I_{\overline{W}^n_{\mathcal{Z}}}(F_n(B_n);Z^n,E_n|F_n)$, we evaluate $I_{\overline{W}_n}(F_n(B_n);Z^n,E_n|F_n)$:

$$\begin{aligned}&\mathbf{E}_{f_n}\exp(\rho I_{\overline{W}_n}((F_n(B_n);Z^n,E_n|F_n = f_n,\Lambda=\lambda))\\ =&\mathbf{E}_{f_n}\exp(\rho\sum_e P_{E_n}(e)I_{\overline{W}_n}(F_n(B_n);Z^n|F_n = f_n,E_n=e,\Lambda=\lambda))\\ \le&\mathbf{E}_{f_n}\sum_e P_{E_n}(e)\exp(\rho I_{\overline{W}_n}(F_n(B_n);Z^n|F_n = f_n,E_n=e,\Lambda=\lambda))\\ \le&1+\sum_e P_{E_n}(e)e^{n\rho(R_{\mathrm{s}}-R_{\mathrm{p}})}\sum_{b,z}P_{B_n}(b)P_{Z^n|B_n,E_n,\Lambda=\lambda}(z|b,e)^{1+\rho}\\ &P_{Z^n|E_n=e,\Lambda=\lambda}(z)^{-\rho}\ \text{(by Eqs. (4–6))}\\ =&1+\sum_e P_{E_n}(e)e^{n\rho(R_{\mathrm{s}}-R_{\mathrm{p}})}\sum_{v,z}\underbrace{\sum_{b:\lambda(b,e)=v}P_{B_n}(b)}_{=P_{V^n|E_n=e,\Lambda=\lambda}(v)}\\ &\underbrace{P_{Z^n|B_n,E_n,\Lambda=\lambda}(z|b,e)^{1+\rho}}_{=P_{Z^n|V^n,\Lambda=\lambda}(z|v)^{1+\rho}}P_{Z^n|E_n=e,\Lambda=\lambda}(z)^{-\rho}\\ =&1+\sum_e P_{E_n}(e)e^{n\rho(R_{\mathrm{s}}-R_{\mathrm{p}})}\sum_{v,z}P_{V^n|E_n=e,\Lambda=\lambda}(v)\\ &P_{Z^n|V^n,\Lambda=\lambda}(z|v)^{1+\rho}P_{Z^n|E_n=e,\Lambda=\lambda}(z)^{-\rho}\\ =&1+\sum_e P_{E_n}(e)\exp(n\rho(R_{\mathrm{s}}-R_{\mathrm{p}})+\psi(\rho,P_{Z^n|V^n,\Lambda=\lambda},P_{V^n|E_n=e,\Lambda=\lambda})\\ =&1+\sum_e P_{E_n}(e)\exp(n\rho(R_{\mathrm{s}}-R_{\mathrm{p}})+\psi(\rho,P_{Z^n|V^n},P_{V^n|E_n=e,\Lambda=\lambda})\\ =&1+\sum_e P_{E_n}(e)\exp(n\rho(R_{\mathrm{s}}-R_{\mathrm{p}})+\psi(\rho,\overline{W}_n,P_{V^n|E_n=e,\Lambda=\lambda}))\\ \le&1+\sum_e P_{E_n}(e)\exp(n\rho(R_{\mathrm{s}}-R_{\mathrm{p}})+\phi(\rho,\overline{W}_n,P_{V^n|E_n=e,\Lambda=\lambda}))\\ &\text{(by Eq. (10))}.\end{aligned}$$

We shall average the above upper bound over Λ. By the almost same argument as [15], we can see

$$\begin{aligned}&\exp(\rho\mathbf{E}_{f_n,\lambda}I_{\overline{W}_n}(F_n(B_n);Z^n,E_n|F_n = f_n,\Lambda=\lambda))\\ =&\exp(\rho\mathbf{E}_{f_n,\lambda}\sum_e P_{E_n}(e)I_{\overline{W}_n}(F_n(B_n);Z^n|F_n = f_n,\Lambda=\lambda,E_n=e))\\ \le&\mathbf{E}_{f_n,\lambda}\exp(\rho\sum_e P_{E_n}(e)I_{\overline{W}_n}(F_n(B_n);Z^n|F_n = f_n,\Lambda=\lambda,E_n=e))\\ \le&1+\mathbf{E}_\lambda\sum_e P_{E_n}(e)\exp(n\rho(R_{\mathrm{s}}-R_{\mathrm{p}})+\phi(\rho,\overline{W}_n,P_{V^n|E_n=e,\Lambda=\lambda}))\\ \le&1+\exp(n\rho(R_{\mathrm{s}}-R_{\mathrm{p}}))\sum_{u\in\mathcal{U}^n}P_{U^n}(u)\exp(\phi(\rho,\overline{W}_n,P_{V^n|U^n=u}))\\ =&1+\varepsilon_{n,\rho}(\overline{W}_n,P_{V^n,U^n}),\end{aligned} \qquad (26)$$

where $\varepsilon_{n,\rho}(\overline{W}_n, P_{V^n,U^n}) := \exp(n\rho(R_{\rm s} - R_{\rm p}) + \phi(\rho, \overline{W}_n, P_{V^n|U^n}, P_{U^n})))$. Taking the logarithm, we have

$$
\begin{aligned}
&\mathbf{E}_{f_n,\lambda} I_{\overline{W}_n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda) && (27)\\
\le& \frac{1}{\rho}\log(1 + \varepsilon_{n,\rho}(\overline{W}_n, P_{V^n,U^n})), && (28)
\end{aligned}
$$

Observe that what we have shown is that the averages over f_n and λ of $\exp(\rho I_{\overline{W}_n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda))$ and $I_{\overline{W}_n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda))$ are smaller than Eqs. (26) and (28).

Let $p(n)$ be a polynomial function of n. We can see that with probability of $1 - 1/p(n)$ the pair (f_n, λ) makes $\exp(\rho I_{\overline{W}_n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda))$ and $I_{\overline{W}_n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda)$ smaller than $p(n)$ times Eqs. (26) and (28), respectively. Since the inequalities (13) and (14) hold at least with probability $1 - \frac{3}{16} = \frac{13}{16}$ with random selection of Λ [10, Eq. (24)], one can take $p(n) > 2\frac{16}{13}|\mathcal{W}_n(Q_V)|$ [3], and by doing so we can see that there exists at least one pair of f_n and λ such that all elements $\overline{W}_n \in \mathcal{W}_n(Q_V)$ satisfies the inequalities (13) and (14) and

$$
\begin{aligned}
&I_{\overline{W}_n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda)\\
\le& \frac{p(n)}{\rho}\log(1 + \varepsilon_{n,\rho}(\overline{W}_n, P_{V^n,U^n})) \le \frac{p(n)}{\rho}\varepsilon_{n,\rho}(\overline{W}_n, P_{V^n,U^n}) && (29)\\
&\exp(\rho I_{\overline{W}_n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda))\\
\le& p(n)(1 + \varepsilon_{n,\rho}(\overline{W}_n, P_{V^n,U^n})). && (30)
\end{aligned}
$$

Thus, (24), (25), (22) and (29) yield that

$$
\begin{aligned}
&I_{\overline{W}_{\mathcal{Z}}^n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda)\\
\le& \sum_{\overline{W}_n \in \mathcal{W}_n(Q_V)} \lambda(\overline{W}_n)\frac{p(n)}{\rho}\varepsilon_{n,\rho}(\overline{W}_n, P_{V^n,U^n})\\
\le& \sum_{\overline{W}_n \in \mathcal{W}_n(Q_V)} \frac{p(n)(n+1)^{|\mathcal{U}|^2|\mathcal{V}|}}{\rho}\varepsilon_{n,\rho}(\overline{W}_{\mathcal{Z}}^n, Q_{V,U}^n)\\
\le& \frac{p(n)|\mathcal{W}_n(Q_V)|(n+1)^{|\mathcal{U}|^2|\mathcal{V}|}}{\rho}\varepsilon_{n,\rho}(\overline{W}_{\mathcal{Z}}^n, Q_{V,U}^n)\\
=& \frac{\overline{p}(n)}{\rho}\varepsilon_{1,\rho}(\overline{W}_{\mathcal{Z}}, Q_{V,U})^n, && (31)
\end{aligned}
$$

where $\overline{p}(n) := p(n)(n+1)^{|\mathcal{U}|^2|\mathcal{V}|}|\mathcal{W}_n(Q_V)|$.

Since $\log\varepsilon_{1,\rho}(\overline{W}_{\mathcal{Z}}, Q_{V,U}) = R_{\rm s} - R_{\rm p} + \phi(\rho, \overline{W}_{\mathcal{Z}}, Q_{V|U}, Q_U)$, for an arbitrary $\delta > 0$, we can choose a large integer n_1 such that

$$
\begin{aligned}
&\inf_{1/n \le \rho \le 1} \log(\frac{\overline{p}(n)}{\rho}\varepsilon_{1,\rho}(\overline{W}_{\mathcal{Z}}, Q_{V,U})^n)\\
\le& \inf_{1/n \le \rho \le 1} \log(\varepsilon_{1,\rho}(\overline{W}_{\mathcal{Z}}, Q_{V,U})^n) + \log\overline{p}(n) + \log n\\
\le& -n(F_+^{\mathcal{I}}(W, R_{\rm p}, R_{\rm s}, Q_{UV}, \Xi) - \delta)
\end{aligned}
$$

for $n \ge n_1$. Since (31) holds with any $\rho \in [1/n, 1]$, we obtain

$$
\begin{aligned}
&\log I_{\overline{W}_{\mathcal{Z}}^n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda)\\
\le& -n(F_+^{\mathcal{I}}(W, R_{\rm p}, R_{\rm s}, Q_{UV}, \Xi) - \delta) && (32)
\end{aligned}
$$

for $n \ge n_1$.

Since $x \mapsto \exp(x)$ is convex, (24), (25), (22) and (30) yield that

$$
\begin{aligned}
&\exp(\rho I_{\overline{W}_{\mathcal{Z}}^n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda))\\
\le& \sum_{\overline{W}_n \in \mathcal{W}_n(Q_V)} \lambda(\overline{W}_n)\exp(\rho I_{\overline{W}_n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda))\\
\le& \sum_{\overline{W}_n \in \mathcal{W}_n(Q_V)} \lambda(\overline{W}_n)p(n)(1 + \varepsilon_{n,\rho}(\overline{W}_n, P_{V^n,U^n}))\\
\le& \sum_{\overline{W}_n \in \mathcal{W}_n(Q_V)} p(n)(1 + \varepsilon_{n,\rho}(\overline{W}_{\mathcal{Z}}^n, P_{V^n,U^n}))\\
\le& p(n)|\mathcal{W}_n(Q_V)|(1 + \varepsilon_{n,\rho}(\overline{W}_{\mathcal{Z}}^n, P_{V^n,U^n}))\\
\le& \overline{p}(n)(1 + \varepsilon_{n,\rho}(\overline{W}_{\mathcal{Z}}^n, Q_{V,U}^n)).
\end{aligned}
$$

Taking the logarithm, we have

$$
\begin{aligned}
&I_{\overline{W}_{\mathcal{Z}}^n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda)\\
\le& \frac{\log\overline{p}(n)^2(1 + \varepsilon_{n,\rho}(\overline{W}_{\mathcal{Z}}^n, Q_{V,U}^n))}{\rho}\\
\le& \frac{\log(2\overline{p}(n)^2)}{\rho} + n\frac{[\log\varepsilon_{1,\rho}(\overline{W}_{\mathcal{Z}}, Q_{V,U})))]_+}{\rho}. && (33)
\end{aligned}
$$

Since $\lim_{\rho\to 0}\frac{[\log\varepsilon_{1,\rho}(\overline{W}_{\mathcal{Z}}, Q_{V,U})))]_+}{\rho} = F_-^{\mathcal{I}}(W, R_{\rm p}, R_{\rm s}, Q_{UV}, \Xi)$, we can choose an integer n_2 such that

$$
\begin{aligned}
&I_{\overline{W}_{\mathcal{Z}}^n}(F_n(B_n); Z^n, E_n | F_n = f_n, \Lambda = \lambda)\\
\le& \text{RHS of(33) with } \rho = 1/\sqrt{n}\\
\le& n(F_-^{\mathcal{I}}(W, R_{\rm p}, R_{\rm s}, Q_{UV}, \Xi) + \delta) && (34)
\end{aligned}
$$

for $n \ge n_2$

Therefore, using (32), (34), we can see that ($F^{\rm s}$, $F^{\rm c}$, $F_+^{\mathcal{I}}$) $F_-^{\mathcal{I}}$) is a universally attainable quadruple of exponents in the sense of Definition 10. ■

Remark 12: By suitably changing $R_{\rm p}$, Q_{UV} and Ξ in Eqs. (16)–(19), the coding scheme used in the proof can achieve a rate triple ($R_{\rm s}$, R_e, $R_{\rm c}$) if there exists a Markov chain $U \to V \to X \to YZ$ and

$$
\begin{aligned}
R_{\rm s} &\le I(V;Y|U), && (35)\\
R_{\rm c} &\le \min[I(U;Y), I(U;Z)],\\
R_e &\le I(V;Y|U) - I(V;Z|U),\\
R_e &\le R_{\rm s}.
\end{aligned}
$$

Observe that Eq. (35) does not exist in Theorem 2, and that our achievable region could be smaller. The reason behind this difference is that we do not split the confidential message into the private message B_n and the common message E_n encoded by the BCD encoder. The coding scheme for BCC in [5] uses this kind of message splitting.

However, when $R_e = R_{\rm s}$, our coding scheme can achieve the rate pairs given in Corollary 3 by suitably changing $R_{\rm p}$, Q_{UV} and Ξ in Eqs. (16)–(19), because the message splitting is unnecessary when $R_e = R_{\rm s}$.

IV. Conclusion

In this paper, we presented universally attainable error and information exponents universally attainable equivocation rates for discrete broadcast channels with confidential messages. The result is novel as far as the authors know. However, there are still rooms for improving this research result. Körner and Sgarro also clarified upper bounds on the error exponents, but we could not obtain one, because it is difficult to evaluate the smallest possible mutual information leaked to Eve over all the possible coding schemes. On the other hand, the non-universal information exponent appeared in [8] is better than one presented here. This suggests that our universally attainable information exponent could be improved.

Acknowledgment

The first author would like to thank Dr. Jun Muramatsu and Prof. Tomohiro Ogawa for the helpful discussion on the universal coding. A part of this research was done during the first author's stay at the Institute of Network Coding, the Chinese University of Hong Kong, and he greatly appreciates the hospitality by Prof. Raymond Yeung. This research was partially supported by the MEXT Grant-in-Aid for Young Scientists (A) No. 20686026 and (B) No. 22760267, and Grant-in-Aid for Scientific Research (A) No. 23246071. The Center for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme.

References

[1] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[2] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. System Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979.

[3] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Budapest, Hungary: Akadémiai Kiadó, 1981.

[4] I. Csiszár, "Almost independence and secrecy capacity," *Problems of Information Transmission*, vol. 32, no. 1, pp. 40–47, 1996.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[6] R. G. Gallager, *Information Theory and Reliable Communication*. New York: John Wiley & Sons, 1968.

[7] M. Hayashi, "General non-asymptotic and asymptotic formulas in channel resolvability and identification capacity and its application to wiretap channel," *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1562–1575, Apr. 2006, arXiv:cs/0503088.

[8] ——, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inform. Theory*, vol. 57, no. 6, pp. 3989–4001, June, 2011.

[9] M. Kobayashi, Y. Liang, S. Shamai (Shitz), and M. Debbah, "On the compound MIMO broadcast channels with confidential messages," in *Proc. IEEE ISIT 2009*, Seoul, Korea, Jun. 2009, pp. 1283–1287, arXiv:0906.3200.

[10] J. Körner and A. Sgarro, "Universally attainable error exponents for broadcast channels with degraded message sets," *IEEE Trans. Inform. Theory*, vol. 26, no. 6, pp. 670–679, Nov. 1980.

[11] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. Inform. Theory*, vol. 23, no. 1, pp. 60–64, Jan. 1977.

[12] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 142374, 2009.

[13] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. Hanover, MA, USA: NOW Publishers, 2009.

[14] R. Matsumoto and M. Hayashi, "Secure multiplex coding with a common message," in *Proc. 2011 IEEE ISIT*, Saint-Petersburg, Russia, Jul. 2011, to appear, arXiv:1101.4036.

[15] ——, "Strong security and separated code constructions for the broadcast channels with confidential messages," 2011, submitted to IEICE Trans. Fundamentals, arXiv:1010.0743.

[16] ——, "Secure multiplex network coding," in *Proc. IEEE NetCod 2011*, Beijing, China, Jul. 2011, to appear, arXiv:1102.3002.

[17] Y. Soma, "On universal wiretap channel coding," Master's thesis, University of Electro-Communications, Jan. 2010, (in Japanese).

[18] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.